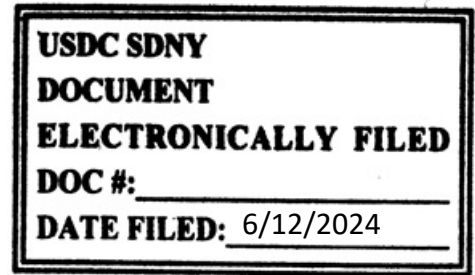


UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK



-----X  
UNITED STATES OF AMERICA,

Plaintiff,

20-CV-2593 (ALC) (KHP)

-against-

ANTHEM, INC.,

**ORDER**

Defendant.  
-----

**KATHARINE H. PARKER, United States Magistrate Judge:**

This case, brought by the U.S. government against Anthem, Inc. (“Anthem”) pursuant to the False Claims Act (“FCA”), asserts that Anthem knowingly disregarded its duty to ensure the accuracy of certain information it submitted to the Centers for Medicare and Medicaid Services (“CMS”), a part of the U.S. Department of Health and Human Services (“HHS”), resulting in it being paid more than it was entitled to for its insurance programs for Medicare recipients.

A core part of the information to be exchanged in this case is the protected health information of Anthem’s members (i.e., patient’s medical information and records). At issue is the level of security needed to protect the health data that is turned over to the government in discovery and who should pay for the costs of that security.<sup>1</sup> The government has proposed a robust set of protections for the data including that the data will be housed on a bespoke platform, not connected to the internet, accessible by only ten individuals—all of whom are U.S. citizens who have been subject to a criminal background check. The system does not allow for

---

<sup>1</sup> The parties do not dispute the level of protection being provided for other types of information produced in discovery and each side is bearing the costs of protecting the other information each receives (e.g., security in place to protect emails reviewed and produced on a review platform such as Relativity).

transfer of data; rather, the only way to transfer data is encrypted physical storage initiated by one of three authorized persons. Additionally, all data is encrypted at the file level and would remain encrypted if it were somehow removed from the platform. The security system proposed by the government is HITRUST-certified.<sup>2</sup> The monthly cost already being incurred by the government for this level of security is about \$5,000/month.

Anthem agrees that the platform has many protections in place but states that it needs additional protections—most that would come into play in the event of a future data breach—which will cost an additional \$4,300/month. The specific additional protections sought include tracking and logging of all activity on the platform, not just tracking and logging data moving in or out of the system; monitoring of internal activity logs; certain data loss prevention controls to mitigate potential security gaps in transfer protocols; and certain measures to address security vulnerabilities exploited in the Microsoft “Midnight Blizzard” cyber-attack. *See* ECF 216-1, Declaration of Chandrasekhar Nagasundaram Vice President, Technology-Cybersecurity for Anthem. Anthem contends the additional measures it is seeking are consistent with industry standards and with applicable regulatory guidance.

The issue of data security in discovery and how costs should be allocated for same is one that does not appear to have been addressed in any other court decision.

Under the federal rules, there is a presumption that the responding party bears the expense of complying with and responding to discovery requests and of preserving its own

---

<sup>2</sup> HITRUST stands for Health Information Trust Alliance—an organization governed by representatives from the healthcare industry that provides a certifiable framework to help healthcare organizations and their providers protect sensitive health information in keeping with legal/regulatory requirements.

information for litigation. *Oppenheimer Fund Inc. v. Sanders*, 437 U.S. 340, 358 (1978). Who should bear the cost of maintaining the security of data turned over in litigation is a slightly different question. It is typical for Courts to issue protective orders governing discovery, but those orders do not usually address secure storage of data or who bears the costs of protecting electronically stored information produced in discovery. Rather, those orders typically describe the process for designating information confidential, challenges to designations, individuals authorized access to confidential information, and the return or destruction of information at the conclusion of the litigation.

Nonetheless, the undersigned's model protective order includes the following:

"Any Personally Identifying Information ("PII") (e.g., social security numbers, financial account numbers, passwords, and information that may be used for identity theft) exchanged in discovery shall be maintained by the receiving party in a manner that is secure and confidential and shared only with authorized individuals in a secure manner. The producing party may specify the minimal level of protection expected in the storage and transfer of its information. In the event the party who received PII experiences a data breach, it shall immediately notify the producing party of same and cooperate with the producing party to address and remedy the breach. Nothing herein shall preclude the producing party from asserting legal claims or constitute a waiver of legal rights and defenses in the event of litigation arising out of the receiving party's failure to appropriately protect PII from unauthorized disclosure."

Accordingly, the protective order in this case contains this language and allows the producing party to specify the minimum level of security expected. See ECF No. 96. It does not address cost-shifting in the event the receiving party disputes the level of protection specified by the producing party.

The Court is mindful of the increasing data security risks faced by law firms and entities in litigation.<sup>3</sup> In 2022, the American Bar Association reported that 27% of law firms reported having experienced a security breach.<sup>4</sup> IBM Security issued a report in 2023 indicating that the average cost of a data breach is more than \$4 million. IBM Security, “Cost of a Data Breach Report 2023.” <https://www.ibm.com/reports/data-breach> (last visited June 11, 2024). And, indeed, there already has been a data breach in this case. Specifically, one of the government’s vendors experienced a ransomware attack that compromised some of Anthem’s data, resulting in the vendor having to send notice to impacted individuals, pay for two-years of credit monitoring, and a lawsuit. ECF No. 96 ¶3. Accordingly, Anthem is rightfully concerned about the protection of its data in this case. Further, HHS has recognized that healthcare information is frequently a target of cyberattacks and care must be taken to protect health information.<sup>5</sup>

Federal Rule of Civil Procedure 26(c)(1)(B) grants the court discretion to allocate expenses for disclosure or discovery upon a showing of “good cause.” The Court in *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 323 (S.D.N.Y. 2003), set forth various factors to aid courts in analyzing which party should bear the cost of electronic discovery. Those factors include: 1) “the extent to which the request is specifically tailored to discover the relevant information”; 2) “the availability of such information from other sources”; 3) “the total cost of production, compared to the amount in controversy”; 4) “the total cost of production, compared to the

---

<sup>3</sup> <https://nysba.org/hackers-working-for-lucrative-cyber-attack-industry-see-law-firms-as-rich-targets/> (last visited June 11, 2024)

<sup>4</sup> [https://www.americanbar.org/groups/law\\_practice/resources/tech-report/2022/cybersecurity/](https://www.americanbar.org/groups/law_practice/resources/tech-report/2022/cybersecurity/) (last visited June 11, 2024)

<sup>5</sup> [www.aspr.hhs.gov/cyber/documents/Healthcare.Sector.Cybersecurity](https://www.aspr.hhs.gov/cyber/documents/Healthcare.Sector.Cybersecurity), Introduction to the Strategy of the U.S. Department of Health and Human Services (“HHS”) (last visited June 11, 2024).

resources available to each party”; 5) “the relative ability of each party to control costs and its incentive to do so”; 6) “the importance of the issues at stake in the litigation”; and 7) “the relative benefits to the parties of obtaining information.” 217 F.R.D. 322. These factors were developed over twenty years ago in the infancy of electronic discovery and before 2006 amendments to the Rules designed to address issues raised by difficulties in “locating, retrieving, and providing discovery of some electronically stored information.” Advisory Committee Notes, 2006 Amendment to Rule 26(b)(2). Thus, these factors are informative, but are not all directly relevant to the question of whether a producing party who wishes a certain level of data security be provided for data produced in discovery can require the receiving party to bear the full cost of such data security protections for the duration of the litigation until the data is destroyed or returned.<sup>6</sup>

In most cases, the receiving party will bear the costs of maintaining the security of data and the risk of a data breach, as each side will receive data and will need to protect that data pursuant to the terms of any protective order and the level of security and costs will be similar for both sides. Additionally, there are strong financial and reputational incentives for parties and their lawyers to ensure the security of the data they receive in discovery. Nevertheless, there may be some instances when it is appropriate to shift certain costs of data security.

---

<sup>6</sup> Courts have referenced these factors in determining cost shifting in similar contexts, however. See, e.g., *IME Watchdog, Inc. v. Gelardi*, 22 Civ. 1023, 2022 WL 2316137 (E.D.N.Y. June 28, 2022)(finding *Zubulake* factors were consistent with finding that the parties should share the cost of forensic examination of electronic devices); *In the Matter of the Complaint of Specialist LLC*, 16 Civ. 5010, 16 Civ. 2515, 16 Civ. 3353, 16 Civ. 3579, 16 Civ. 4643, 16 Civ. 7001, 2016 WL 6884919 (recognizing the party possessing information normally must bear the expense of preserving it for litigation but nevertheless shifting costs of preservation of physical evidence – a ship – and noting that *Zubulake* factors, while not necessarily directly applicable, were consistent with shifting costs).

Further, there may be different levels of security needed for different types of information produced in a litigation.

After careful consideration, the Court has identified the following, non-exclusive factors as relevant to determining whether there is good cause to shift all or a portion of costs of data security measures from the receiving party to the producing party: 1) the nature of the information to be protected and risks and costs associated with unauthorized disclosure of such information; 2) the reasonableness of the security measures requested by the producing party (which can include an evaluation of the degree of risk mitigated by the security requested relative to less costly security measures); 3) the cost of the data security requested relative to the overall costs of discovery and amount in controversy; and 4) relative ability of the parties to pay the costs of the security requested by the producing party. These factors are not necessarily entitled to the same weight in every case and should be balanced based on the particulars of each case.

As to factor one, the information sought to be protected here is medical information and related personally identifying information about individuals who are not parties to this litigation. This type of information is often the subject of cyber attacks, and includes deeply personal details about the non-parties included in the data set. This data has already been the subject of a cyber attack in this case, meaning that it is a high risk target of future cyber attacks. The costs associated with compromise of this information are high because of the number of people who could be affected by a security breach. Further, the costs associated with addressing a large security breach are in the millions of dollars. Given these risks, and

particularly given the previous breach, Anthem's concern for the security of the data is reasonable and this factor weighs against shifting the costs of that security to Anthem.

As to factor two, the security requested by Anthem is the security requested of all of its vendors and thus not unusual nor newly calculated to cause hardship to the Plaintiff. On the other hand, the system proposed by the government is already secure and takes into account health industry standards for protection of information. Additionally, unlike with Anthem's regular vendors, the information will not be accessible via the internet, is encrypted and will be accessible to only 10 people. It is not clear how much additional risk will be mitigated from the additional measures proposed by Anthem. Ultimately, the only technical opinion offered by the parties is from Anthem's head of Cybersecurity Threat Management, whose declaration identifies specific vulnerabilities in the government's proposal. The Court can not rely on the representations of lawyers for the government to conclude that their proposed safeguards are sufficient. Therefore, this factor also weighs against shifting the costs of data security to Anthem.

As to factor three, the cost of the additional data security measures is about \$60,000 per year, which would nearly double the Government's data-hosting and security costs. At the same time, the Government is alleging that Anthem unlawfully obtained and retained millions of dollars in payments. ECF No. 26-1. Therefore, the annual costs of the additional security measures are a rounding error relative to the entire amount in controversy, and this factor also weighs against shifting the costs of data security to Anthem.

As to factor four, both sides have an ability to pay the cost of the additional security, but they are not equally resourced. Anthem has retained a global law firm to defend this action, O'Melveny, whose associates regularly bill at rates about \$500/hour, and whose partners bill at rates exceeding \$1000/hour. *See e.g., Mogan v. Sacks, Ricketts & Case LLP*, 2022 WL 1458518, at \*2 (N.D. Cal. May 9, 2022)(listing rates charged by O'Melveny counsel and partners.) It generates billions of dollars in revenues and has significant resources to defend this action. The Department of Justice also is well-resourced, but the Court is mindful that it is financed by tax dollars and pursuing this case to recover public funds it asserts were overpaid to Anthem. Nevertheless, the disparity in resources and source of those resources is not so great, especially in light of the total cost of litigation and amount in controversy, as to raise concerns that the producing party (Anthem) is seeking to make prosecuting the case against it financially untenable. On the whole, this factor weighs slightly in favor of shifting the costs of data security to Anthem, but not as strongly as in a situation where there is a greater financial disparity between the parties.

After considering all of these factors, the Court finds that the additional security measures requested by Anthem are proportionate to the nature of the information sought to be protected, reasonable in light of the only evidence provided on the level of security required, and proportionate to the total amount in controversy and the overall costs of litigation. While Anthem is slightly better positioned to absorb these additional costs, that factor alone does not outweigh the others particularly where there has already been a data breach due to the

requesting party's prior insufficient protections. Accordingly, the government has not shown good cause to shift the burden to Anthem to pay for the additional security requested.

### **CONCLUSION**

For the reasons set forth above, Plaintiff shall implement the additional security measures requested by Anthem and bear the cost of the additional security measures. However, this decision is without prejudice to a renewed motion under Rule 26 to shift the costs of this enhanced security if Defendant engages in conduct that unreasonably extends discovery so as to increase the costs to Plaintiff. *See e.g., Est. of Shaw v. Marcus*, 2017 WL 825317, at \*6 (S.D.N.Y. Mar. 1, 2017)(noting discovery-related misconduct was relevant to analysis of whether discovery cost-shifting was appropriate). It is also without prejudice as to any rights the government may have as a prevailing party to recover costs.

**SO ORDERED.**

New York, New York  
June 12, 2024



---

Katharine H. Parker  
U.S. Magistrate Judge